AUTHORIZATION CODE RECOVERING METHOD

The present invention relates to a method for recovering an authorization code, which was assigned to a licensee by a licensor, with the authorization code being stored in an access-protected data-processing device, which is connected to a computer of the licensor via an interface.

Application programs, software, and other electronic documents are often protected from unauthorized access. To use this electronic data and these programs, the user needs a license from the licensor. The licensee receives an authorization code, which enables him to exercise his license, from the licensor.

In the simplest case, the authorization code is sequence of alphanumeric characters, which is input manually by the licensee during the first use of the program or for each opening of a document. However, one disadvantage of this method is that the licensee can pass on the authorization code to unauthorized third parties, so that it can lead to undesired duplication of the authorization code and thus to misuse of the license.

Alternatively, the authorization code can be stored directly by the licensor in a data-processing device known as a dongle. The authorization code cannot be removed from the dongle; thus it cannot be duplicated. The execution of a computer program protected in this way is possible only if the dongle is connected to an interface of the computer on which the application program is to be executed. Because the dongle is created by the licensor, a separate dongle, which occupies the interface on the computer, is necessary for each application program. If the dongle is lost or destroyed, the licensor must be contacted in order to create a new dongle with the corresponding authorization code and send it to the licensee.

Electronic data-processing devices on which several authorization codes are stored for application programs or digital documents are also known. These devices are also connected to the interface of a computer. One example for such a data-processing device is the codemeter stick made by Wibu Systems AG. This is a mobile license stick, which is connected, for example, to the USB interface of a computer. The principle and operation of such a licensing device are described in EP 1 184 771 B1.

A licensee purchases an "empty" data-processing device. The licenses or "digital rights" can be written onto the data-processing device only by the originators or authorized licensors. The owner of the device can neither create nor write licenses or authorization codes of a licensor into the device by himself independently.

On the data-processing device, "digital rights" from several independent licensors can be stored for several different and independent products. These can also be, in addition to

application programs and computer software, documents, music files, or films. The licenses can be of various types, for example, unrestricted in time, restricted in time, or restricted in use, so-called pay-per-use licenses or the like. As soon as the stick is inserted into the computer, the corresponding programs can query the authorization codes of the licenses and enable use or access.

The greater the number of authorization codes and digital rights stored in the device, the greater the value of the device. If a device in which many licenses or authorization codes for licenses are stored is lost or damaged, the restoration of the authorization codes is very labor-intensive. For each individual license, the corresponding licensor must be contacted; proof of the authorization and the purchase of the licenses must be provided and sent to the licensor. This is a complicated and long procedure. Often, it is not possible recover all of the authorization codes. For use-dependent licenses, which decrease with the frequency of use, the licensor is usually not ready to restore the license completely.

Thus, the task of the present invention is to restore authorization codes stored securely in a device to be connected to the computer simply and quickly in the case of a lost or defective device.

The present invention is realized by a method according to the characterizing features of Claim 1. Preferred improvements of the method according to the invention are defined in subordinate Claims 2-10.

The method according to the invention for restoring an authorization code that was assigned to a licensee by a licensor, with the authorization code being stored in an access-protected data-processing device connected to a computer of the licensee via an interface, accesses a security file stored on the computer of the licensee. The security file belonging to the authorization code contains the license parameters for the corresponding authorization code. According to the method according to the invention, the following steps are performed:

Reading the parameters belonging to the licensor from the security file stored on the computer. Establishing a remote data connection between the computer of the licensee and a computer of the licensor and sending the read license parameters to the computer of the licensor. Furthermore, then the authorization code corresponding to the received license parameters are restored by the licensor. The licensor sends the restored authorization code back to the computer of the licensee. In the last step, the restored authorization code is stored in the data-processing device connected to the computer of the licensee.

The authorization code is an access code or an access authorization in order to be able to execute a program or access digital data. The digital data includes, for example, films, music files, or other protected documents. Thus, the authorization code represents a "digital right" to be able to use files licensed by the originator in the scope of an existing license. In addition, the

authorization code also includes all of the license parameters necessary for restoring the authorization code. Only with the appropriate authorization code protected on a data-processing device is it possible to store the license parameters in a security file on the computer.

In order to restore the authorization code stored on the device, a security file stored on the computer is needed. Thus, there is a clear separation between the memory location of the security file and the location, at which the authorization code is stored. In the case of a lost or destroyed data-processing device, the security file remains available on the computer. The security file also includes, in addition to the license parameters, other information that enables it to contact the licensor. The license parameters include all of the data required for restoring the authorization code. In addition, additional information on the licensee can also be stored in the security file. Because the security file does not contain the authorization code itself, no special protection of the security file is necessary. It can be copied or duplicated.

The creation or updating of the security file can be initiated by a licensed application or executed manually or automatically periodically. As a standard, it is created automatically every 24 h. Thus, a very up-to-date security file is always available. This is especially important for restoring authorization codes for time-dependent or use-dependent licenses. An existing security file is updated at the latest when new licenses or authorization codes are requested or license parameters are updated by the licensor.

For a lost or damaged data-processing device, a new data-processing device is obtained by the licensee and connected to the interface of the computer. However, the new data-processing device is "empty" and contains absolutely no license data. Thus, the original authorization code must be restored to this new device. For restoring the lost authorization code, the license parameters required for restoring the authorization code are sent to the licensor. The licensor evaluates the received license parameters. On the basis of the "old" license parameters, the licensor restores the authorization code or generates a "new" authorization code. The new or restored authorization code then corresponds to the authorization code protected on the original device. The licensor remains the only authorized party for generating the authorization code. Thus, he has the control over every issued and generated authorization code for the licenses granted by him; thus it remains his decision whether he restores the authorization code or not.

The restored authorization code is sent to the licensee, for example, via the Internet. Here, the code can be encrypted for transmission. Transmission in other ways, for example, by writing onto a diskette or CD and mailing the diskette or CD, is also conceivable.

However, the received authorization code cannot be stored in the computer of the licensee itself, but instead only in the connected data-processing device. Thus, the computer establishes only a connection, for example, an Internet connection, and passes on the authorization code to the data-processing device. If a new data-processing device is not

connected to the interface of the computer, then the entire method for restoring the authorization code cannot be performed and the Internet connection between the computer of the licensee and the computer of the licensor is broken.

The method is also suitable for transmitting an authorization code from a first device to a second device. For this purpose, a delete command is also sent to the first device in order to delete the authorization code to be transferred from the device. Otherwise, the authorization code would be duplicated. However, this is not desired by the licensor.

According to the invention, the authorization code is preferably stored in a device-specific format in the data-processing device. Thus, the code can be stored only on the device, but not on the connected computer establishing the connection to the licensor. To the computer, the device-specific format in which the authorization code is provided is unreadable. Therefore, it can also neither be copied nor can it be manipulated or modified by a user or licensee. Thus, the storage of the authorization code is very secure against unauthorized access.

Advantageously, the license parameters in the security file are present at least partially in encrypted form and are stamped with the date and time of creation. Sensitive license parameters can be protected against access by third parties through encryption. In particular, confidential data, such as personal data of the licensee or data containing the authorization for the receipt or possession of an authorization code, is encrypted. However, the entire security file can also be encrypted. The electronic signature ensures that the license parameters cannot be changed. In the case of manipulation of the license parameters or the security file, the signature and the data no longer match. Thus, misuse of the security file is reliably ruled out, as is manipulation of the license parameters. This is especially important because the security file can be copied.

In addition, the license parameters belonging to an authorization code can be encrypted by the licensor and transmitted signed to the licensee. Then the license parameters also cannot be manipulated by unauthorized third parties during the exchange between the licensee and the licensor.

In addition, the security file is stamped with a time signal. The stamping is realized with the last certified time of the data-processing device. During production, the data-processing device receives a certified time. When the data-processing device is connected to the interface of a computer, this time is always counted forwards. Thus, it corresponds to neither the current time nor the system time of the computer. However, it is advantageous that this certified time cannot be manipulated. Furthermore, this time can be updated with time certificates delivered by time servers via the Internet.

Especially preferred is an improvement of the method in which the following additional steps are executed: receiving the license parameters at the licensor and then evaluating the

license parameters. On the basis of the evaluated parameters, in the next step it is decided whether the requested authorization code should be restored and sent back to the licensee.

Thus, the licensor decides freely and according to his own business whether an authorization code shall be restored. Especially for repeated losses or repeated requests for restoring the authorization code, the licensor can deny the restoration. If the loss of one or more devices at periods very close in time is reported by a licensee, the licensor can delay restoration dependent on further testing or can completely refuse restoration.

The licensor can also decide in which way the restoration is to be performed depending on the license issued to the licensee. This is especially important when the license is a time-restricted license, a use-restricted license, so-called pay-per-use license, or some other special license. Only the licensor decides whether the authorization code is restored identically or in a modified form. For so-called pay-per-use license models, in which the digital rights contain so-called units of use, similar to a charge card, the licensor can decide to restore a percentage of its value, depending on how old the security file of the licensee is.

Preferably, the security file that had been assigned to the owner of the device contains certified time information. The security file then obtains a digital stamp with time information in order to rule out manipulation of the time of the creation of the security file.

Advantageously, the additional steps can also be performed: sending time information stored in the security file to the licensor, evaluating the time information by the licensor and generating an authorization code corresponding to the time information.

The time information contained in the security file can provide the time of the creation of the security file. At the time at which the security file was created, the device reported as lost or defective with the included authorization code was still functional and connected to the computer. For time-dependent licenses, the authorization code can now be restored as a function of the time information. Here, deviating from the originally provided license, a modified authorization code can be generated and sent to the licensee. If the time limit of the time-restricted license has expired in the interim, the restoration of the authorization code is refused. For use-dependent licenses, only a percentage of the use allotment can be made available by the licensor in the restored authorization code as a function of the contained time information.

Certified time information is encrypted and transmitted to the data-processing device from the licensor. This can be performed when the licensee establishes a connection to the licensor. However, the certified time information can also be requested from a special time server as soon as the computer to which the data-processing device is connected has established a connection to the Internet.

It is especially advantageous when several authorization codes for licenses of several licensors are stored on the data-processing device. The greater the number of authorization codes

stored on the data-processing device, the higher the value that the data-processing device represents. Thus, the restoration of lost or damaged authorization codes is especially important. The larger the number of authorization codes and different licensors, the more complicated is the creation of authorization codes in the case of a lost or destroyed data-processing device. In this case, for each license and for each licensor, a separate set of license parameters is stored in the security file.

Preferably, a connection to all licensors is established in order to allow the corresponding authorization codes to be restored. The licensors are stored in the security file. Each licensor receives only the data set of license parameters that are necessary for creating the authorization code of the license issued by him. He receives absolutely no information on other licenses, other authorization codes, or other licensors. Thus, information on other programs, data, music files, or films used by the same licensee remains in the private sphere of the licensee. Because the individual licensor receives only his license parameters from the security file, he can also restore only his licenses. This represents an additional security aspect in the restoration of authorization codes.

For restoring all authorization codes, the individual licensors stored in the security file are contacted individually and one after the other in order to request the authorization codes for the issued licenses. The method according to the invention is executed several times. The licensee must provide neither the data nor the addresses of the individual licensors. He does not have to know exactly whether and which type of licenses he possesses. Also, the licensee does not have to know when and where these licenses were purchased.

In the method according to the invention, in an especially preferred way the following additional steps are performed: establishing a remote data connection between the computer of the licensee and a central management computer, sending the security file to the management computer, and establishing a data connection between the computer of the licensor and the central management server.

The entire security file is sent to the central management computer during the process of restoring one or more authorization codes. The management server then reads the license parameters and the licensor from the security file and establishes the connection between the licensor or licensors and the management server. The management server manages the entire restoration of the authorization code or codes. Especially if there were many authorization codes from different licensors on the lost data-processing device, the use of the management server enables a quick and convenient restoration of all of the authorization codes. The management server can contact the individual licensors optionally one after the other and request the restoration of the authorization codes belonging to the licenses. After receiving the authorization code from the licensors, it can pass on the authorization codes to the licensee.

Preferably, in another step a remote data connection to the computer of the licensee and the computer of the licensor is established. If authorization codes from several licensors are stored on the data-processing device, all of the licensors stored in the security file are contacted and a connection to them is created. The return of the restored authorization codes can take place directly from the licensor to the licensee. The management server no longer must be connected in-between. In this way, first, the management server is relieved of administrative tasks, and, second, the restoration process can be significantly accelerated.

Furthermore, an improved method, in which the security file contains an unmodifiable serial number of the data-processing device, is especially preferred. If a security file is written, simultaneously the internal serial number of the data-processing device is also stored in the security file. The serial number is here preferably stored in a non-manipulatable format.

Preferably, the following additional steps are also executed: the serial number is read from the security file and sent to a management server. The serial number received by the management server is then stored in a block list in the management server. With each execution of the restoration of an authorization code, the serial number of the original data-processing device on which the authorization codes were stored is transmitted to the management server. The original data-processing device is thus reported as defective, lost, or stolen and registered in the block list. In this way, a list is created with all of the data-processing devices, the authorization codes of which were restored. Thus, unauthorized continued use of a lost or defective device can be prevented. Misuse of the restoration process as a duplicating process for authorization codes is thus ruled out.

If an Internet connection is established by the licensee's computer, to which a data-processing device with an authorization code is connected, then a signal can be sent to the management server. Also, if a certified time signal is to be queried from the management server or a time server, for example, in order to update the time information in the security file, the Internet connection to the computer of the licensee is recognized. The data-processing device then sends its serial number to the management server via the computer of the licensee. The management server tests the received serial number with the block list managed by it for defective or lost devices. If the received serial number of the data-processing device has already been stored in this number list, then a block notice is stored on the data-processing device in the form of a flag, which blocks the device and the retrieval of the protected authorization code. The data-processing device can then no longer be used. In this way, misuse of the restoration method is prevented. Duplication of the authorization code with the aid of the restoration process is thus stopped.

Alternatively, the licensor can also store the serial number of a data-processing device reported as lost or stolen in a number list. The licensor also sends the serial number of the device

reported as stolen or defective to a management server that manages a list with all of the devices reported stolen. The management server checks whether the transmitted serial number originates from an authorized licensor. If this is the case, the serial number is recorded in the list. The database managed by the management server with the blocked serial numbers can be queried by every authorized licensors and certified time servers.

If a licensor receives a request to restore an authorization code, he first checks the transmitted serial number. For this purpose, he queries the database of blocked serial numbers of the management server. If the serial number is not contained in the database, the restoration process of the authorization code continues.

If the transmitted serial number is contained as a blocked number in the list, then a block signal is sent to the corresponding data-processing device. The data-processing device is then blocked and can no longer be used; the authorization codes stored on it can no longer be used. Any type of decryption or authentication is thus prevented.

A special embodiment of the invention is explained in more detail with reference to the following figures. Shown are:

Figure 1, the security structure on the side of the licensee for two data-processing devices;

Figure 2, the process sequence for requesting and storing restored authorization codes on a new data-processing device.

For two data-processing devices 1, 1' in Figure 1, a security file 2, 2' is assigned to each. For this purpose, the creation of a security file is initiated by an application program, a so-called back-up manager 3. The back-up manager 3 creates the security files 2, 2' as a function of parameters in a security control file 4.

Figure 2 shows the process for storing the restored authorization codes in a new data-processing device 5. If the data-processing device 1 is lost or defective, the security file 2 is read by the back-up manager 3. All of the license parameters contained in this file are evaluated by the back-up manager 3 in a first step S1.

In the second step S2, the license parameters belonging to the first licensor 6 are transmitted to the licensor 6. The licensor 6 generates an authorization code corresponding to the authorization code stored in the data-processing device 1 on the basis of the received license parameters. The restored authorization code is then transmitted in a third step S3 to the back-up manager 3.

In the fourth step S4, a remote data connection to the licensor 7 is established and the corresponding license parameters are transmitted to it. The licensor 7 restores the authorization codes corresponding to the received license parameters and returns them in step S5 to the back-up manager 3. In the subsequent steps S6 and S7, this method is repeated for the licensor 8.

The back-up manager 3 passes on the authorization codes received from the licensors 6, 7, 8 in another step S8 to the new data-processing device 5 and stores these codes there. The data-processing device 5 now contains all of the authorization codes that were stored in the defective data-processing device 1. Here, the restoration of the authorization codes that were stored in the security file 2 was requested from all of the licensors 6, 7, and 8.

List of reference symbols

1, 1' Data-processing device
2, 2' Security file
3 Back-up manager
4 Security control file
5 Data-processing device
6, 7, 8 Licensor

Claims

1. Method for restoring an authorization code assigned to a licensee by a licensor, with the authorization code being stored in an access-protected data-processing device (1, 1'), which is connected to a computer of the licensee via an interface, characterized in that
a security file (2, 2'), which belongs to the authorization code and which contains the license parameters, is stored on the computer of the licensee, and

the following steps are executed:

reading of the license parameters belonging to the licensor (6, 7, 8) from the security file (2, 2');

sending the read license parameters to the licensor (6, 7, 8);

restoring the authorization code corresponding to the received license parameters at the licensor (6, 7, 8);

returning the restored authorization code to the computer of the licensee;

storing the restored authorization code in the data-processing device (5) connected to the computer of the licensee.

2. Method according to Claim 1, characterized in that the authorization code is stored in a device-specific format in the data-processing device.

3. Method according to Claim 1 or 2, characterized in that the license parameters are signed with time information for protection and are provided at least partially in encrypted form in the security file (2, 2').

4. Method according to one of Claims 1 to 3, characterized by the following additional steps:

receiving the license parameters at the licensor (6, 7, 8);

evaluating the license parameters;

deciding whether the requested authorization code should be restored and returned to the licensee.

5. Method according to one of Claims 1 to 4, characterized by the following additional steps:

sending time information stored in the security file (2, 2') to the licensor (6, 7, 8);

evaluating the time information by the licensor (6, 7, 8);

generating an authorization code corresponding to the time information.

6. Method according to one of Claims 1 to 5, characterized in that several authorization codes for licenses of several licensors (6, 7, 8) are stored on the data-processing device (1, 1', 5).

7. Method according to one of Claims 1 to 6, characterized in that remote data connections are established to all licensors (6, 7, 8), in order to permit the corresponding authorization codes to be restored.

8. Method according to one of Claims 1 to 7, characterized by the following additional steps:

establishing a remote data connection between the computer of the licensee and a central management computer;

sending the security file (2, 2') to the management server;

establishing a data connection between the computer of the licensor (6, 7, 8) and the central management server.

9. Method according to Claim 8, characterized by the additional step:
establishing a remote data connection between the computer of the licensee and the computer of the licensor (6, 7, 8).

10. Method according to one of Claims 1 to 9, characterized in that
the security file (2, 2') contains an unmodifiable serial number of the data-processing device (1, 1', 5) and the following additional steps are executed:

reading the serial number from the security file (2, 2');

sending the serial number to a management server;

storing the serial number in a block list at the management server.